Information management Policy

FRDC

Managing Director's authorisation: Patrick W Hone

Effective date: 26 April 2018

TABLE OF CONTENTS

1. PURPOSE

The purpose of this policy is to provide direction to employees on the creation and management of corporate information.

2. RESPONSIBILITY

Responsibility for this policy resides with the General Manager Business.

3. DEFINITIONS AND ACRONYMS

Definitions - follow link to Definitions
Acronyms – follow link to Acronyms and Abbreviations

4. RISK CATEGORY

Compliance	Financial	Governance	ICT	People	Research
□	□	☒	□	□	□

5. RELEVANT DOCUMENTATION

This section contains links to internally and externally facing documents – access to internally facing documents is restricted to FRDC employees.

Relevant documentation	Document location or web address
Internal	
Records management Policy	NEMO-17805-62
Records management procedure	NEMO-29-1565
External	
Digital Continuity Policy (NAA) 2020	Digital continuity policy
Managing information (NAA)	NAA
Protective Security Policy	Protective security policy
Information Governance Framework	Information Governance Framework

6. PUBLICATION

This policy is to be made available on the FRDC website.
This policy is not to be made available on the directors' site.

7. BACKGROUND

FRDC's information is a corporate asset, vital both for ongoing operations and also in providing valuable evidence of business decisions, activities and transactions.

FRDC is committed to establishing and maintaining information practices that meet its business needs, accountability requirements, and stakeholder expectations. FRDC is also committed to the principles and practices set out in whole-of-government policies and best-practice standards.

The benefits of compliance with this policy will be trusted information that is well-described, stored in known locations, and accessible to employees and clients when needed.

This policy applies to FRDC employees and contractors, to all aspects of the business and all business information created and received. It covers information in all formats including documents, email, voice messages, memoranda, minutes, audio-visual materials and business system data. The policy also covers all business applications used to create, manage and store information, including the official information management systems, email, websites, social media applications, databases and business information systems. This policy covers information created and managed in-house and off-site.

8. POLICY

FRDCs data, information, and records management processes will reflect best practice standards, and comply with the following legislation and regulatory requirements:

- AS/NZS ISO 9001:2015 Quality Management Systems
- National Archives of Australia – Digital Continuity Policy 2020
- Protective Security Policy – Mandatory Requirements

The FRDC will implement fit-for-purpose information management systems and practices to ensure the creation, maintenance and protection of reliable information.

FRDC management will ensure that storage mechanisms for corporate information maintain, and ensure the integrity of the source information. Where applicable, the source data format will be maintained (e.g. email message, Secure PDF, etc), as well as the related metadata.

Employees will create and capture business information in endorsed information systems. Business information created should provide a reliable and accurate account of business decisions and actions. Employees will include all necessary information to support business needs including the names, dates and time, and other key information needed to capture the business context.

Employees will classify all business information created or captured so as to:

- store the content/information in the appropriate system or storage medium
- provide users with a positive experience when searching for, or finding information
- provide context for business activities
- enable the implementation of retention or records declaration policies, based on specific object metadata
- meet FRDCs' external commitments and obligations

If content cannot be classified for any reason, employees will use the title/name/unique identifier for the object to provide as much information as reasonable in its classification.

FRDC management will ensure that FRDC systems allow:

- information to be received into the correct information lifecycle management process
- its security to be maintained for its intended audience

- it to be used in a fashion that is aligned with the intention of the owner
- objects/transactions to be managed in line with relevant policies

Information is a corporate resource to which all employees may have access, except where the nature of the information requires restriction. Access restrictions will not be imposed unnecessarily but will protect:

- individual employees, or client privacy
- sensitive material such as security classified material or material with dissemination limiting markings, for example 'Commercial in Confidence'

When sharing corporate information externally, a number of additional factors will be taken into account. FRDC employees will ensure the:

- security of the information is maintained, and only shared with authorised external parties, or marked in such a way as to specify its business classification
- information is relevant to the intended audience
- information does not open FRDC up to an increased risk profile
- information to be shared has the approval of the content owner, or specific business manager
- source information still exists within approved systems and maintains its integrity

Corporate information will be managed throughout its lifecycle, and part of this management is to ensure information is retained for at least the required length of time. Information storage will align to FRDCs' obligations and commitments, supported by strong audit trails. Part of the purpose for retention is to maintain the context, metadata, and integrity of the information in all forms. Information maintenance will safeguard changes to information when:

- information is transferred or migrated to new/other systems, platforms, or applications
- is shared with internal or external parties
- is transferred from physical mediums such as paper, to digital formats

FRDC management may destroy information when it reaches the end of its required retention period as set out in records authorities issued by the National Archives of Australia. However, some information can be destroyed in the normal course of business. This is information that is low value, of a short-term, facilitative or transitory value that is destroyed as a 'Normal Administrative Practice'. Examples of such information includes rough working notes, drafts not needed for future use, duplicated or copies of information held for reference or 'for information only'.

Employees will not destroy information, other than in accordance with FRDC's policies and procedures, without the approval of the General Manager Business.

Unauthorised destruction risks penalties under the Archives Act, and may expose FRDC to a range of other risks including:

- an inability to comply with regulatory and legislative responsibilities such as the Freedom of Information Act 1982 and the Privacy Act 1988;
- an inability to provide access to information requested by legal discovery action; and
- damage to organisational reputation

FRDC does not prescribe to a single Electronic Document and Records Management System (eDRMS) for the management of corporate information, but rather a collection of applications and services that are integrated and support the requirements of this policy. The approved applications and storage mediums include:

- Microsoft Office 365 and its subset of services
- Microsoft Dynamics 365

FRDC management will ensure all employees maintain the required skills and practices around information management. FRDC will honour this commitment by:

- providing regular training for all employees on changes to information management requirements, and supporting procedures
- developing efficient and effective business processes, which limit ambiguity and manual handling of information
- providing help and supporting information in a variety of forms; for users to reference when required

9. ATTACHMENTS

#	**Description**
Nil	